

## **REMARKS**

### **Claim Status**

Claims 1-21 are now pending, with claims 1 and 10-18 being in independent form. Claims 1-18 have been amended. Independent claims 12, 14, 16 and 18 have been placed into independent form. Dependent claims 19-21 have been added. The amendments to claims 2-9 are merely cosmetic or clarifying in nature. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

### **Information Disclosure Statement**

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry and acknowledgment that the IDS and the reference cited therein have been entered and considered is requested.

### **Overview of the Office Action**

Claims 10-18 have been objected to based on a minor informality. Withdrawal of this objection is in order, as also explained below.

Claims 10-18 stand rejected under 35 U.S.C. §101 as directed to non-statutory subject matter.

Claims 1-18 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,845,447 ("*Fujioka*").

Applicants have carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now presented for examination in the instant application are patentable over the cited art.

### **Descriptive Summary of the Prior Art**

*Fujioka* relates to “an electronic voting system and method for implementing secure secret voting in elections, questionnaire surveys or the like which are conducted through a telecommunication system” (see col. 1, lines 8-11).

### **Summary of the Claimed Subject Matter**

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The specification discloses an efficient and secure electronic voting scheme based on fair blind signatures. In a fair blind signature scheme (*FBSS*), there is an additional participant, one or more trusted authorities (or “judges”), and the signer can identify which signature resulted from a given signing session with the help of the trusted authority (or a quorum of trusted authorities if there is more than one).

If the signer has a transcript of a particular signing session, it then becomes possible to identify the signature-message pair resulting from that session. Conversely, if a particular signature-message pair is available to the signer, then the signer can determine the particular signing session at which this was generated.

Fair blind signature schemes enable a given digital signature to be linked to a given user, while retaining the privacy of the user’s message. The claimed invention thus provides a way to determine the authenticity of a particular vote, while still permitting the actual vote of the voter to remain private.

### **Amendments Addressing Informalities**

The Examiner has objected to claims 10-18 for the inclusion of numerals in each claim. In response to this objection, applicants have amended claims 10-18 to delete the numerals in parentheses from each of these claims. Withdrawal of the objection is therefore deemed to be in order.

### **Patentability of the Independent Claims under 35 U.S.C. 101**

The Examiner (at pg. 3 of the Office Action) has stated that claims 12, 14, 16 and 18 are directed to a computer product and are, therefore, directed to non-statutory subject matter. The Examiner (at pg. 3-5 of the Office Action) has also stated that claims 10, 11, 13, 15 and 17 are directed to software and are, thus, directed to non-statutory subject matter.

With respect to the rejection of claims 12, 14, 16 and 18, applicants thank the Examiner for his suggested language. In any event, applicants have amended claims 12, 14, 16 and 18 to place them into independent form, such that claims 12, 14, 16 and 18 now recite a “computer readable medium encoded with a computer program executed by a computer that causes...”. Independent claims 12, 14, 16 and 18 now also recite that the computer program includes the program code for executing the corresponding features recited in claims 10, 13, 15 and 17, respectively.

With respect to claims 10, 11, 13, 15 and 17, applicants have amended these claims in the manner suggested by the Examiner.

In view of the foregoing, independent claims 10-18 as now amended are directed to statutory subject matter, reconsideration and withdrawal of the rejection under 35 U.S.C. §101 are accordingly deemed to be in order, and notice to that effect is requested.

### **Patentability of the Independent Claims under 35 U.S.C. §102(e)**

Independent claims 1 and 10-18 have been amended to clarify the salient features of the claimed invention. That is, independent method claim 1 has been amended to recite the steps of “obtaining from a signer apparatus, using a fair blind signature scheme, a digital signature ( $y_i$ ) of a data signal ( $x_i$ ) from a voter apparatus, said data signal comprising a vote ( $v_i$ ) of the voter; and establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme”. Independent claims 10-18 have been amended to recite corresponding limitations. Thus, each independent claim clarifies features associated with the use and implementation of a fair blind digital signature. No new matter has been added.

*Fujioka* (col. 2, lines 24-29) explains that it is an object “to provide a simple and convenient electronic voting system and method which ensure voter privacy in making a complaint about a possible fraud by the administrator, have robustness against system dysfunction and obviate the necessity for voters to send their encryption keys to the counter after voting”. According to *Fujioka*, “[t]he election administrator verifies the validity of the voter through utilization of his signature attached to the encrypted text, then attaches a blind signature to the preprocessed text, and sends back the signed preprocessed text to the voter. The voter excludes the influence of the random number from the blind signature attached to the preprocessed text to obtain administrator’s signature information about the encrypted vote content, and sends the signature information as vote data to the counter together with the encrypted vote content” (see col. 2, lines 36-46).

Amended independent claims 1 and 10-18, on the other hand, each recite a “fair blind signature scheme”. The blind signature of *Fujioka* is a different concept than and is differently implemented from that associated with the use of a fair blind signature implemented as recited in independent claims 1 and 10-18 in which a trusted authority apparatus is enabled to establish a link between a given digitally-signed data signal and a signing session. *Fujioka* thus fails to teach or suggest the step of “establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme,” as recited in now amended independent claim 1 and correspondingly recited in now amended independent claims 10-18.

As explained at pg. 2, lines 18-20 of the specification as originally filed, the claimed invention provides “an efficient and secure electronic voting scheme based not on ordinary blind signatures but on fair blind signatures”. As additionally explained at pg. 2 of the instant specification, “[i]n an ordinary blind signature scheme, if the signer signs a number of documents for different users then, when he is presented with one particular document that he has signed, he will not be able to determine when or for whom he signed that document. By way of contrast, in a fair blind signature scheme (*FBSS*), there is an additional participant, one or more trusted authorities (or ‘judges’), and the signer can identify which signature resulted from a given signing session with the help of the trusted authority (or of a quorum of trusted authorities if there is more than one)” (see, e.g., lines 21-27 of the specification).

*Fujioka* describes an old, well-known blind signature technique. There is no mention whatsoever in the entire disclosure of the *Fujioka* patent of the word *fair* in association with *blind signature*, i.e., the words “fair blind signature” are not disclosed. *Fujioka* thus fails to teach or

suggest now amended independent claims 1 and 10-18 which each recite the use of a fair blind signature scheme. *Fujioka* fails to teach or suggest the expressly recited subject matter of now amended independent claims 1 and 10-18.

Reconsideration and withdrawal of the rejection of independent claims 1 and 10-18 as anticipated by *Fujioka* under 35 U.S.C. §102 are accordingly deemed to be in order, and early notice to that effect is solicited.

Moreover, by virtue of the above-discussed differences between the recitations of claims 1 and 10-18 and the teachings of *Fujioka*, and the lack of any clear motivation for modifying *Fujioka* to achieve applicants' claimed invention, independent claims 1 and 18 are likewise deemed to be patentable over *Fujioka* under 35 U.S.C. §103.

### **Dependent Claims**

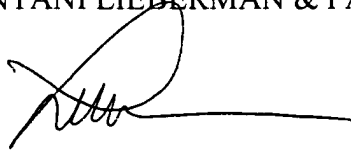
In view of the patentability of independent claims 1 and 10-18 for at least the reasons presented above, each of dependent claims 2-9, as well as each of new dependent claims 19-21, is deemed to be patentable therewith over the prior art. Moreover, each of dependent claims 2-9 and 19-21 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

### **Conclusion**

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

Respectfully submitted,  
COHEN PONTANI LIEBERMAN & PAVANE LLP



By \_\_\_\_\_  
Lance J. Lieberman  
Reg. No. 28,437  
551 Fifth Avenue, Suite 1210  
New York, New York 10176  
(212) 687-2770

Dated: February 27, 2009